AMENDMENTS TO THE CLAIMS

Claims 1-32 are pending in the instant application. Claims 2-4, 7, 8, 11-13, 16, 18, 19, 22, 24, 25, 28 have been amended. The Applicant requests reconsideration of the claims in view of the following amendments reflected in the listing of claims.

Listing of claims:

1. (Original) A method for secure communication of information in a communication network, the method comprising:

acquiring a security code from a second communication device by a first communication device;

receiving media containing said security code from said first communication device;

translating said security code to an IP address corresponding to said second communication device; and

routing said received media to said second communication device based on said IP address of said second communication device, said IP address of said second communication device remaining anonymous to said first communication device.

2. (Currently amended) The method according to claim 1[[2]], wherein said security code is a pin code.

3. (Currently amended) The method according to claim 1, ~~further~~ comprising limiting a duration for which said security code is valid to at least one of time and a number of uses.

4. (Currently amended) The method according to claim 1, ~~further~~ comprising obtaining said acquired security code out-of-band.

5. (Original) A machine-readable storage having stored thereon, a computer program having at least one code section for secure communication of information in a communication network, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

acquiring a security code from a second communication device by a first communication device;

receiving media containing said security code from said first communication device;

translating said security code to an IP address corresponding to said second communication device; and

routing said received media to said second communication device based on said IP address of said second communication device, said IP address of said second communication device remaining anonymous to said first communication device.

6. (Original) The machine-readable storage according to claim 5, wherein said security code is a pin code.

7. (Currently amended) The machine-readable storage according to claim 5, ~~further~~ comprising code for limiting a duration for which said security code is valid to at least one of time and a number of uses.

8. (Currently amended) The machine-readable storage according to claim 5, ~~further~~ comprising code for obtaining said acquired security code out-of-band.

9. (Original) A system for secure communication of information in a communication network, the system comprising:

at least one processor that acquires a security code from a second communication device by a first communication device;

said at least one processor receives media containing said security code from said first communication device;

said at least one processor translates said security code to an IP address corresponding to said second communication device; and

said at least one processor routes said received media to said second communication device based on said IP address of said second communication device, said IP address of said second communication device remaining anonymous to said first communication device.

10. (Original) The system according to claim 9, wherein said security code is a pin code.

11. (Currently amended) The system according to claim 9[[8]], wherein a duration for which said security code is valid is limited in at least one of time and a number of uses.

12. (Currently amended) The system according to claim 9[[8]], wherein said acquired security code is obtained out-of-band.

13. (Currently amended) The system according to claim 9[[8]], wherein said at least one processor is at least one of a server, a media exchange server and a proxy server.

14. (Original) A method for secure communication of information in a communication network, the method comprising:

receiving a security code from a first communication device desiring to communicate with a second communication device;

transferring security information associated with said second communication device to said first communication device;

receiving media along with at least a portion of said transferred security information from said first communication device; and

if said security information from said first communication device is valid, transferring said media from said first communication device to said second communication device.

15. (Original) The method according to claim 14, wherein said security information is a one-time certificate.

16. (Currently amended) The method according to claim 14, wherein said security information ~~further~~ comprises at least one of a device ID, a public key, a code, a device number and a public key.

17. (Original) The method according to claim 14, wherein said security code is transferred out-of-band between said first communication device and said second communication device.

18. (Currently amended) The method according to claim 14, ~~further~~ comprising temporarily storing said received media until said security information received from said first communication device is validated.

19. (Currently amended) The method according to claim 14, ~~further~~ comprising translating said at least a portion of said transferred security information received from said first communication device into an IP address of said second device, said transferring of said media from said first communication device to said second communication device utilizing said IP address of said second device, said IP address of said second communication device remaining anonymous to said first communication device.

20. (Original) A machine-readable storage having stored thereon, a computer program having at least one code section for secure communication of information in a communication network, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving a security code from a first communication device desiring to communicate with a second communication device;

transferring security information associated with said second communication device to said first communication device;

receiving media along with at least a portion of said transferred security information from said first communication device; and

if said security information from said first communication device is valid, transferring said media from said first communication device to said second communication device.

21. (Original) The machine-readable storage according to claim 20, wherein said security information is a one-time certificate.

22. (Currently amended) The machine-readable storage according to claim 20, wherein said security information ~~further~~ comprises at least one of a device ID, a public key, a code, a device number and a public key.

23. (Original) The machine-readable storage according to claim 20, wherein said security code is transferred out-of-band between said first communication device and said second communication device.

24. (Currently amended) The machine-readable storage according to claim 20, ~~further~~ comprising code for temporarily storing said received media until said security information received from said first communication device is validated.

25. (Currently amended) The machine-readable storage according to claim 20, ~~further~~ comprising code for translating said at least a portion of said transferred security information received from said first communication device into an IP address of said second device, said transferring of said media from said first communication device to said second communication device utilizing said IP address of said second device, said IP address of said second communication device remaining anonymous to said first communication device.

26. (Original) A system for secure communication of information in a communication network, the system comprising:

at least one processor that receives a security code from a first communication device desiring to communicate with a second communication device;

said at least one processor transfers security information associated with said second communication device to said first communication device;

said at least one processor receives media along with at least a portion of said transferred security information from said first communication device; and

if said security information from said first communication device is valid, transferring said media from said first communication device to said second communication device.

27. (Original) The system according to claim 26, wherein said security information is a one-time certificate.

28. (Currently amended) The system according to claim 26, wherein said security information ~~further~~ comprises at least one of a device ID, a public key, a code, a device number and a public key.

29. (Original) The system to claim 26, wherein said security code is transferred out-of-band between said first communication device and said second communication device.

30. (Original) The system according to claim 26, wherein said at least one processor temporarily stores said received media until said security information received from said first communication device is validated.

31. (Original) The system according to claim 26, wherein said at least one processor translates said at least a portion of said transferred security information received from said first communication device into an IP address of said second device, said transferring of said media from said first communication device to said second communication device utilizing said IP address of said

second device, said IP address of said second communication device remaining anonymous to said first communication device.

32. (Original) The system according to claim 26, wherein said at least one processor is at least one of a server, a media exchange server and a proxy server.